Threat Analysis of Voting Systems

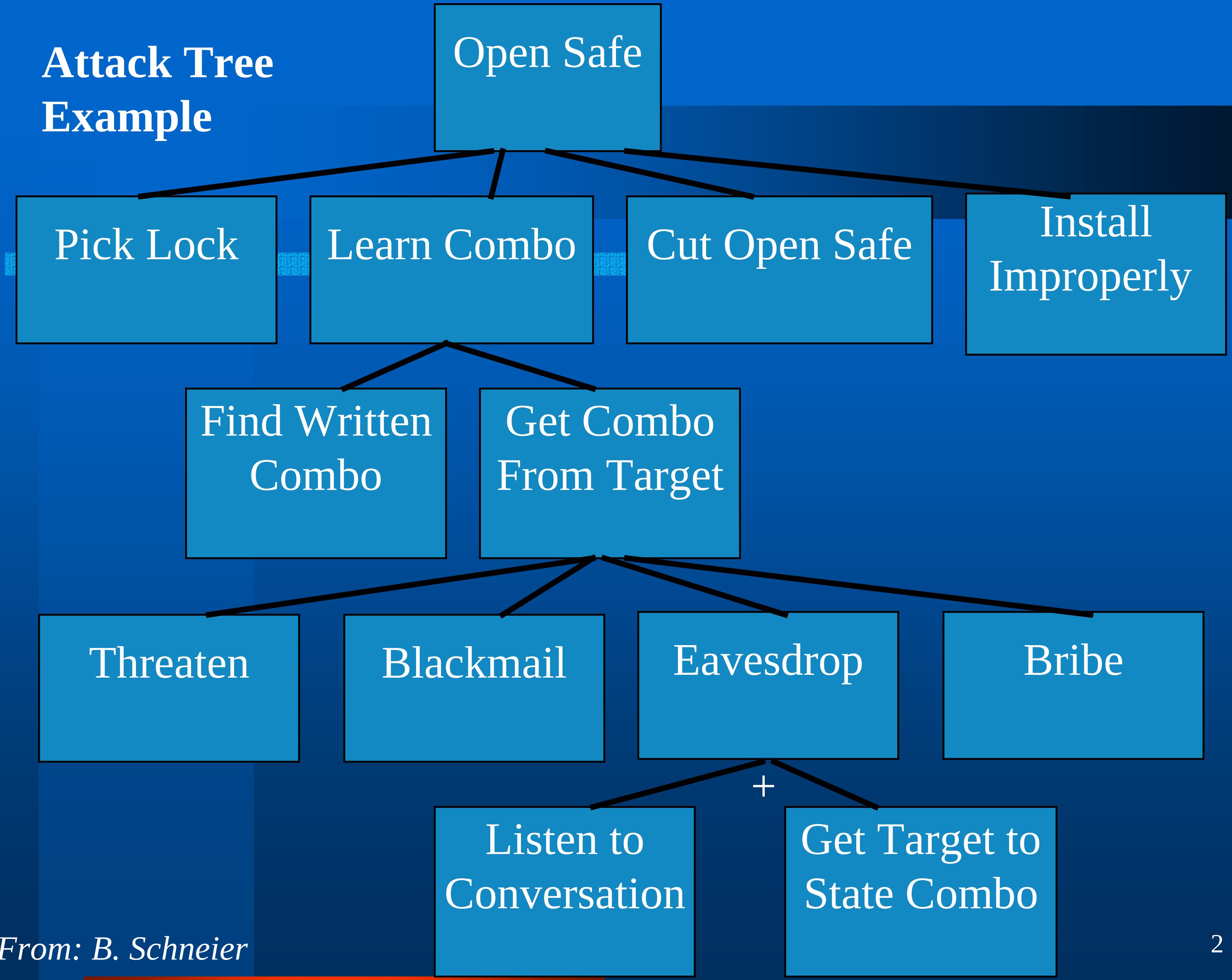
Eric Lazarus Larry Norden

for the

Brennan Center for Justice

at New York University School of Law

Attack Tree Example



Open Safe

Pick Lock

Learn Combo

Cut Open Safe

Install Improperly

Find Written Combo

Get Combo From Target

Threaten

Blackmail

Eavesdrop

Bribe

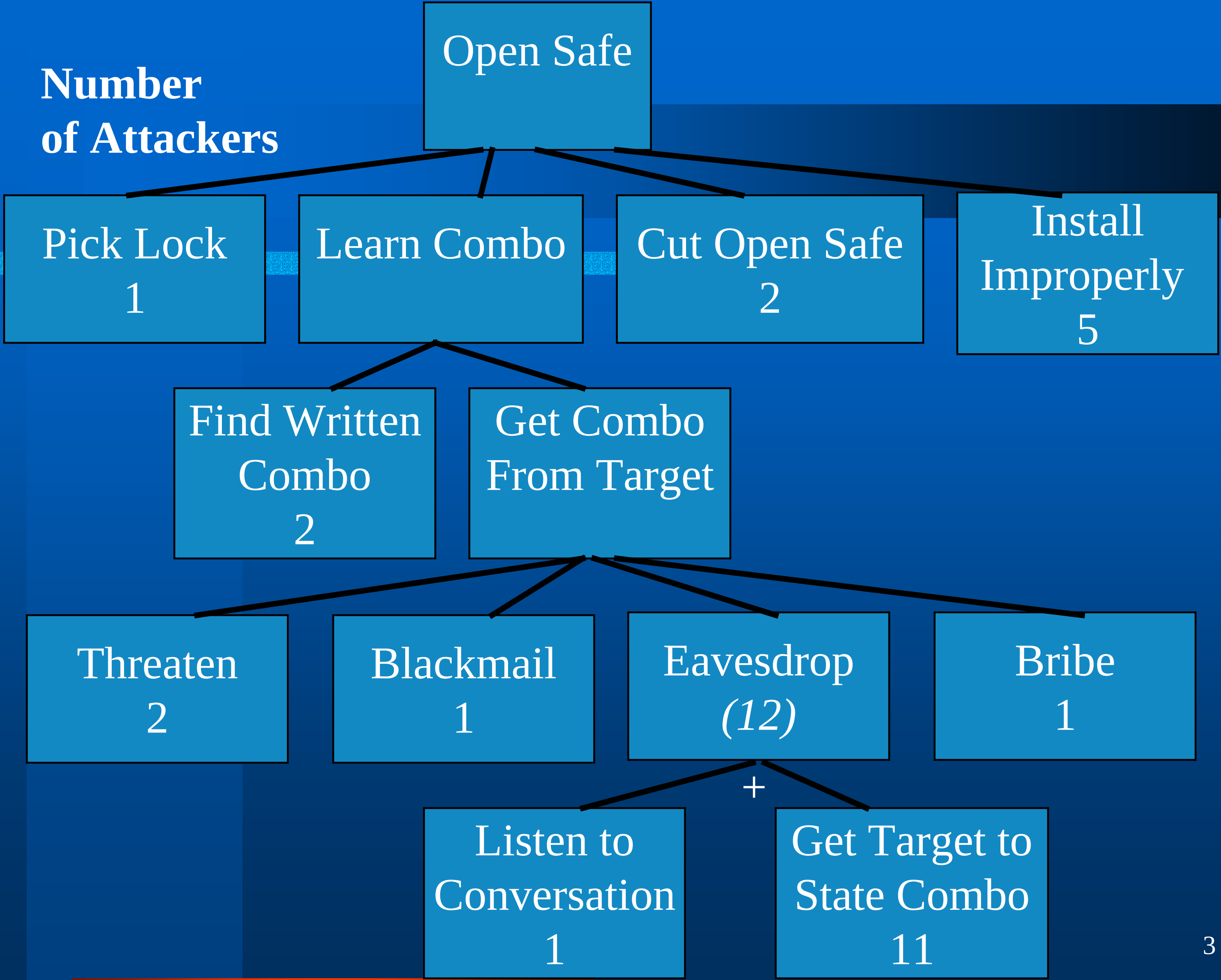
+

Listen to Conversation

Get Target to State Combo

From: B. Schneier

Number of Attackers



Open Safe

Pick Lock
1

Learn Combo

Cut Open Safe
2

Install Improperly
5

Find Written Combo
2

Get Combo From Target

Threaten
2

Blackmail
1

Eavesdrop
(12)

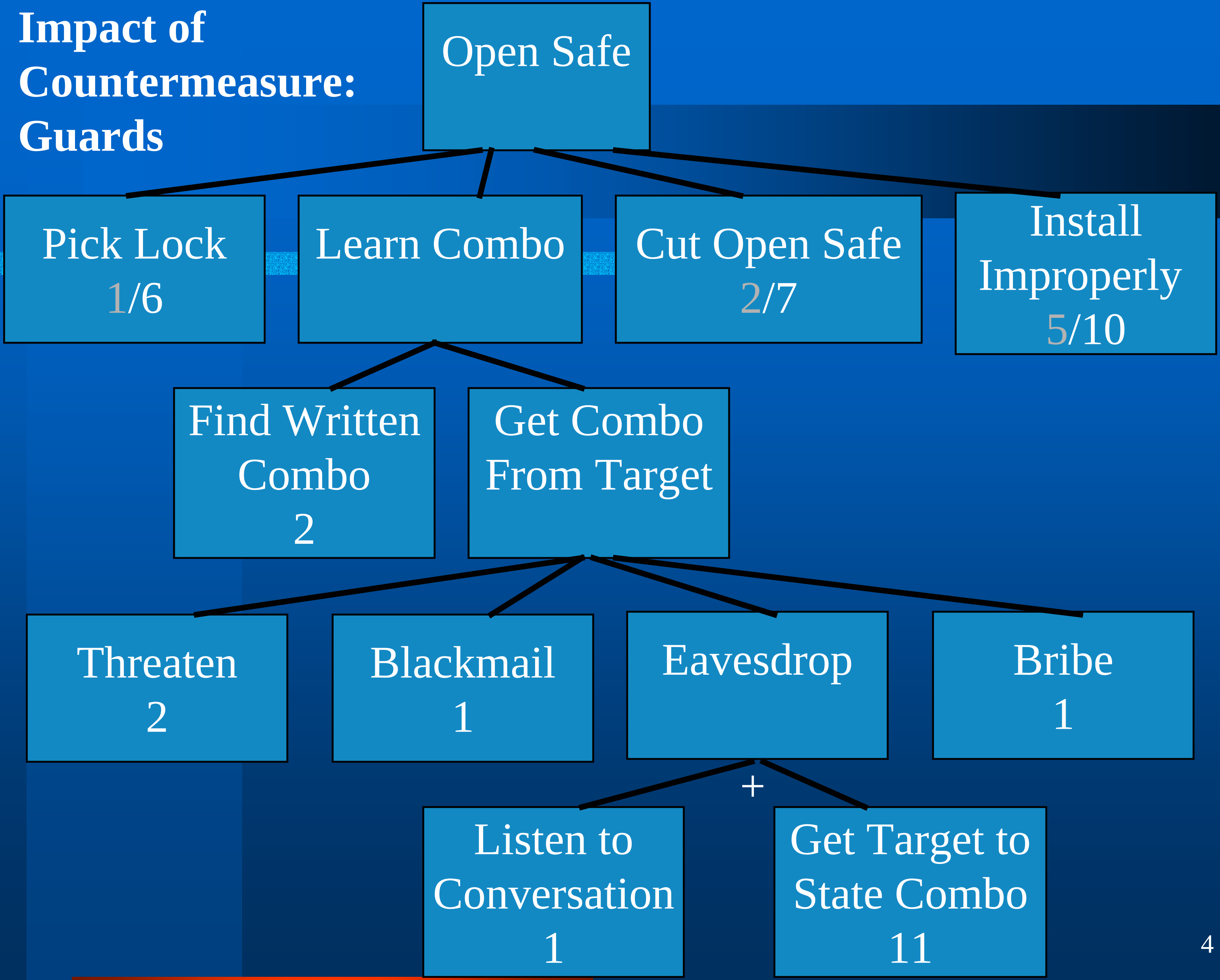
Bribe
1

+

Listen to Conversation
1

Get Target to State Combo
11

Impact of Countermeasure: Guards



Open Safe

Pick Lock
1/6

Learn Combo

Cut Open Safe
2/7

Install Improperly
5/10

Find Written Combo
2

Get Combo From Target

Threaten
2

Blackmail
1

Eavesdrop

Bribe
1

+

Listen to Conversation
1

Get Target to State Combo
11

Other Possible Approaches

- – Measure complexity of the “trusted computing base”
- – Count number of points of vulnerability
- – Measure compliance with accepted security practices
- – Measure how well technology has incorporated NIST Risk Assessment Technical Controls

Attack Team Size as Metric

- Options
  - Cost ($)
  - Elapsed time
  - Total attack team size
  - Co-opted insiders (outsiders are easy to get)

Assumed Jurisdiction/Election

- **Goal: Changing outcome of significant election**
- **Analysis requires**
  - **Which races?**
  - **How close is the attacked race?**
  - **How many votes are targeted?**
  - **How many poll workers per polling place?**
  - **How many polling places are there?**
- **In future, custom analysis**

Which Systems Examined?

- Technology types:
  - DRE
  - DRE with VVPT
  - PCOS
  - BMD
- Selected because common and available in 2006
- Cryptographic systems, witness systems amenable to methodology

Conclusion

- **Feedback on Specific Attacks**
- **Feedback on our Method**